REMARKS

Claims 1, 2, and 4 were presented and examined. In response to the Office Action, Claims 1 and 4 are amended, no claims are cancelled, and no claims are added. Applicants respectfully request reconsideration of pending Claims 1-2 and 4 in view of at least the following remarks.

I. Claims Rejected Under 35 U.S.C. §103

Claims 1, 2, and 4 are rejected under 35 U.S.C. §103 as being unpatentable over U.S. Publication 2004/0205419 to Liang ("Liang") in view of U.S. Publication 2003/0212903 to Porras ("Porras," previously cited) in view of U.S. Patent No. 7,234,168 to Gupta ("Gupta," previously cited) and further in view of U.S. Publication 2007/0079367 to Ishikawa ("Ishikawa," previously cited). Applicant respectfully traverses the aforementioned rejection for the following reasons.

Claim 1 recites:

> 1. A method for detecting abnormal traffic at a network level using a statistical analysis, the method comprising the steps of:
>
> a) gathering local traffic data from each network device and integrating a plurality of the local traffic data to generate traffic data for approximating an overall network traffic level by a single traffic sensing module;
>
> b) extracting a characteristic network traffic data corresponding to the overall network traffic level;
>
> c) comparing the characteristic network traffic data with a predetermined characteristic network traffic data profile resulting from statistical computations and representing normal traffic, and determining whether there is abnormal traffic at the network level;
>
> d) updating the predetermined characteristic traffic data profile using the characteristic traffic data if there is no abnormal traffic in the network, analyzing a volume amount of the abnormal traffic and monitoring the abnormal traffic if there is abnormal traffic at the network level; and
>
> e) transmitting the analysis result of the seriousness of the abnormal traffic to an abnormal traffic processing system to detect abnormal traffic without operation of a network manager, and processing the abnormal traffic to prevent a network failure.

While Applicants' argument here is directed to the cited combination of references, it is necessary to first consider their individual teachings, in order to ascertain what combination (if any) could be made from the cited references.

Regarding the rejection of independent Claims 1 and 4 under 35 U.S.C. 103(a) as being unpatentable over Liang in view of Porras in view of Gupta and further in view of Ishikawa, we are amending Claim 1 to recite:

> "c) comparing the characteristic network traffic data with a predetermined characteristic network traffic data profile resulting from statistical computations and representing normal traffic, and determining whether there is abnormal traffic at the network level; ..." (see claim amendments).

Liang relates to multi-level virus outbreak alerts that are based on collaborative behavior. Liang describes detecting abnormal events in a single client device, and determining whether to adjust an alert level that is sent to a user (see Abstract). Liang is not concerned with overall network traffic levels, but is limited to detecting abnormal activity within a client device (see page 2, paragraph 0011 of Liang) Liang discloses reporting abnormalities if abnormal events are detected in only one client device. As a result, Liang cannot teach the approximation of an overall network traffic level, as in Claim 1. In contrast with Claim 1, Liang does not disclose integrating local traffic data for approximating an overall network traffic level.

As recognized by the Examiner, Liang does not disclose the extraction of characteristic data, as in Claim 1. The Examiner cites Porras as disclosing the characteristic data extraction of Claim 1.

Porras discloses a plurality of service monitors 16A-16C, domain monitors 16D-16E, and enterprise monitor 16F. From all of the monitors, Porras must collect data. That is, Porras does not teach Applicant's amended Claims 1 and 4 recitation of *extracting a characteristic network traffic data corresponding to the overall network traffic level.* The Examiner's reliance on Porras is improper, because it cannot be said that data from a header relates to network traffic data that corresponds to an approximated overall network traffic level, as in Claim 1.

As correctly recognized by the Examiner, Porras fails to teach or suggest a single traffic sensing module, as in Claim 1. As a result, the Examiner cites Gupta, which according to the Examiner, teaches that it is well known to have traffic sensing module and refers to FIG. 2, unit 52, which Gupta refers to as a sensor management module. (See pg. 3, para. 3 of the Office Action mailed 7/1/2008.)

Gupta generally relates to a method of provisioning computers against computer attacks. Gupta describes the constructing of a hierarchy characterizing different computer attacks and counter measures and traversing this hierarchy to identify computer attacks and counter measures relevant to a target platform. As further described by Gupta, the detection and protection measures are then downloaded to a security sensor associated with the target platform. (See col. 2, lines 3-11.) However, rather than disclosing a single traffic sensor module to gather local traffic data and integrate the local traffic data to generate traffic data at a network level, Gupta discloses that local sensor modules 27 may be distributed throughout a network. (See col. 3, lines 35-37.)

Furthermore, the sensor module 52, as shown in FIG. 2 of Gupta, is part of a sensor 22 which is included in each local sensor security module (LSSM). (See FIGS. 1 and 2.) As indicated above, Gupta discloses that the local sensor security modules are distributed throughout the network. (See Supra.) As a result, the Examiner has failed to identify, and we are unable to discern any portion of Gupta which discloses, teaches, or suggests gathering local traffic data from each network device and integrating a plurality of local traffic data to generate traffic data in the network level by a single traffic sensing module, as in Claim 1.

Moreover, none of Liang, Porras or Gupta discloses, teaches, or suggests transmitting the analysis result of the seriousness of the abnormal traffic to an abnormal traffic processing system to detect abnormal traffic without operation of a network manager and processing the abnormal traffic to prevent a network failure, as in Claim I.

As correctly recognized by the Examiner, Gupta fails to teach or suggest detecting abnormal traffic without operation of a network manager and processing the abnormal traffic to prevent a network failure. As a result, the Examiner cites Ishikawa. We disagree with the Examiner's assertions and characterizations regarding Ishikawa.

Ishikawa generally relates to a system and method for detecting, identifying and responding to fraudulent requests on a network. According to the Examiner, the above feature of Claim 1, which is neither taught nor suggested by Porras in view of Gupta, is disclosed by paragraph 41 of Ishikawa. However, paragraph 41 of Ishikawa merely describes abnormal traffic patterns (defined as activity on the network that exceeds predefined acceptable parameters) to a traffic analyzer that monitors the traffic to determine whether the influx of traffic is changing, such as increasing or decreasing, or remaining the same in volume. However, rather than process the abnormal traffic to prevent a network failure, Ishikawa teaches withholding a server network address so that the problematic traffic is no longer directed to a switching device 18. Hence, the combination of Liang in view of Porras, in view of Gupta, and in view of Ishikawa fails to teach or suggest detecting abnormal traffic without operation of a network manager, and processing the abnormal traffic to prevent a network failure, as in Claims 1 and 4.

Furthermore, the Examiner's citing of Ishikawa fails to rectify the deficiency of the combination of Liang in view of Porras in view of Gupta to teach or suggest the comparison of characteristic network traffic data (corresponding to an approximated overall traffic level) with a predetermined characteristic network traffic data profile resulting from statistical computations and representing normal traffic to determine whether there is abnormal traffic at the network level. As disclosed by Porras, a monitor 66 builds a statistical model of network activity from network packets by building long-term and short-term statistical profiles from measures derived from the network packets, such that a monitor can compare the long-term and short-term profiles to detect suspicious network activity (see page 4, paragraph 71 of Porras); however, the updating of the long-term statistical profile is not conditioned on a lack of abnormal traffic in the network, as in Claims 1 and 4.

Hence, no combination of Liang, in view of Porras, in view of Gupta and Ishikawa can disclose, teach, or suggest comparing the characteristic network traffic data with a **predetermined** characteristic network traffic data profile resulting from statistical computations and representing normal traffic, and determining whether there is abnormal traffic at the network level; updating the **predetermined** characteristic network traffic data profile using the characteristic traffic data if there is no abnormal traffic in the network, as in Claims 1 and 4.

In this connection, a predetermined characteristic traffic data profile is described in the specification at page 2, paragraph 0034, from which it is clear that the claimed predetermined characteristic traffic data profile differs from the prior art in that updating of the long-term statistical profile is not conditioned on a lack of abnormal traffic in the network, as in Claims 1 and 4. Moreover, the Examiner has failed to identify, and we cannot discern, any portion of Liang, Porras, Gupta, or Ishikawa that teaches "*a) gathering local traffic data from each network device and integrating a plurality of the local traffic to generate traffic data for approximating an overall network traffic level by a single traffic sensing module; b) extracting a characteristic network traffic data corresponding to the overall network traffic level; c) comparing the characteristic network traffic data with a predetermined characteristic network traffic data profile resulting from statistical computations and representing normal traffic, and determining whether there is abnormal traffic at the network level,*" as in Claim 1. Support for the amendment to Claims 1 and 4 is provided at page 2, paragraph 0019 of Applicant's Specification.

For each of the above reasons, therefore, Claim 1 and all claims which depend from Claim 1, are patentable over the cited art. Consequently, Applicants respectfully request the Examiner reconsider and withdraw the §103(a) rejection of Claims 1 and 2.

Each of Applicant's other independent claims includes limitations similar to those in Claim 1 discussed above. Therefore, all of Applicants' other independent claims, and all claims which depend on them, are also patentable over the cited prior art for similar reasons. Consequently, Applicants respectfully request that the Examiner reconsider and withdraw the §103(a) rejection of Claim 4.

DEPENDENT CLAIMS

In view of the above remarks, a specific discussion of the dependent claims is considered to be unnecessary. Therefore, Applicants' silence regarding any dependent claim is not to be interpreted as agreement with, or acquiescence to, the rejection of such claim or as waiving any argument regarding that claim.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending (1) are in proper form, (2) are neither obvious nor anticipated by the relied upon art of record, and (3) are in condition for allowance. A Notice of Allowance is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207-3800.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly, extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: April 16, 2009

By: ______________________
Joseph Lutz, Reg. No. 43,765

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
Telephone (310) 207-3800
Facsimile (408) 720-8383

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web to the United States Patent and Trademark Office on April 16, 2009.

____
Si Vuong